2006 Interagency Compilation of Federal Privacy and Civil Liberties Policies that Impact Information Sharing*

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
1	**U.S. Constitution – especially Fourth and Fifth Amendments**	Constitu-tion	Provides fundamental individual protections vis-à-vis government.	Yes.	Information sought/ used by USG.	WMD 9.4, Markle, TIA, CDT
2	**Information Sharing, section 1016 of IRTPA, 6 USC 485**	Statute	Establishes "information sharing environment."	Yes – Requires guidelines for protection of privacy and civil liberties.	Terrorism information.	WMD 9.4, AT
3	**Privacy and Civil Liberties Oversight Board, section 1061 of IRTPA, 5 USC 601 note**	Statute	Establishes Board.	Yes – Provides Board with access, advice, oversight authorities and responsibilities relating to privacy and civil liberties.	"[R]elated to efforts to protect the nation from terrorism." Includes terrorism information.	WMD 9.4, AT
4	**National Security Act of 1947, as amended by IRTPA, section 102A and 103A, 50 USC 403-1, 3d**	Statute	Various provisions authorizing/requiring sharing.	Yes – Creation of Civil Liberties Protection Officer position.	National intelligence.	WMD 9.4
5	**Privacy Act, 5 USC 552a, as amended by the Computer Matching and Privacy Protection Act of 1978**	Statute	Privacy Act sets collection, maintenance, and disclosure conditions; access and amendment rights and notice and record-keeping requirements with respect to personally identifiable information retrieved by name or identifier. Computer matching provisions (amending Privacy Act) provide a framework for the intra- and inter-agency comparison of electronic personnel and benefits-related information systems.	Yes, see summary.	Information about a citizen or LPR that contains name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or photograph.	ISWG, OMB, CMS/LGL, Markle, TIA, CDT

*This document was prepared by the Interagency Working Group tasked with preparing the ISE Privacy Guidelines. The research identfied the 109 sets of rules set forth herein. The list is not exhaustive, but may serve as a starting point for agencies to identify the laws and policies applicable to ISE information.

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
6	**E-Government Act of 2002**	Statute	Section 208 requires agencies to analyze (i) how they handle personally identifiable information used in electronic business processes and (ii) where protecting privacy demands modifications to the business process or information system (i.e., Privacy Impact Assessment).	Yes – Requires PIAs and Web site privacy notices; exemption for "national security systems." Also, modification or waiver of PIA is permitted "for security reasons, or to protect classified, sensitive, or private information contained in an assessment."	Information in identifiable form that is collected, maintained, or disseminated by information technology. Does not apply to "national security systems." "Identifiable form" means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.	OMB, CRS, Markle
7	**Freedom of Information Act, 5 USC 552**	Statute	Provides for the disclosure of agency records to the public, subject to certain exemptions.	Yes – Contains exemptions relating to personal privacy information – exemptions 6 and 7(c).	Agency records.	WMD 9.4, ISWG, CRS, CDT,TIA
8	**Foreign Intelligence Surveillance Act (electronic surveillance, physical search, pen registers, business records)**	Statute	Governs collection, retention, dissemination of foreign intelligence information via electronic surveillance, physical search, business records, pen register trap/trace. Requires AG-approved minimization procedures to protect USP information.	Yes – Collection predicates, minimization requirements.	Information acquired under FISA (electronic surveillance, physical search, pen register/trap trace, business records).	ISWG, WMD 9.4, CRS, Markle, TIA, CDT
9	**Pen Registers and Trap and Trace Devices Act, 18 USC 3121 et seq.**	Statute	Provisions on collecting information via pen registers and trap/trace devices.	Yes – Collection predicate.	Communications addressing information.	CRS, TIA
10	**National Security Act of 1947, Patriot Act and Homeland Security Act amendments, 50 USC 403-5b and 5d**	Statute	Patriot Act and Homeland Security Act amendments authorizing and requiring sharing of foreign intelligence collected from criminal investigations.	No.	Information acquired in the course of criminal investigations.	ISWG, CRS
11	**USA Patriot Act, sections 203(a) and (b) – Authority to share Grand Jury Information; Electronic, Wire, and Oral Interception Information**	Statute	Amends Rule 6 to authorize sharing of grand jury information in matters involving FI and CI; Adds (6) to 18 USC 2517, authorizing sharing of information collected via authorized interception with federal law enforcement, intelligence, and other national security officials.	Yes – Use limited to official duties; GJ info requires filing under seal; sharing of USP information subject to AG guidelines.	Information acquired via Grand Jury subpoena or Title III/ECPA.	LSG, CRS, TIA

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
12	**Homeland Security Act of 2002, sections 895 and 896, Authority to share Grand Jury Information; Electronic, Wire, and Oral Interception Information**	Statute	Authorizes sharing of grand jury information for terrorism prevention, etc.; Adds (7) and (8) to 18 USC 2517, authorizing sharing of information collected via authorized interceptions with federal/state/local/foreign officials.	Yes – Use limited to official duties, pursuant to joint AG/DCI guidelines.	Same as above.	
13	**Homeland Security Act of 2002, section 892, Facilitating Homeland Security Information Sharing Procedures**	Statute	Under procedures prescribed by President, requires sharing of homeland security information across federal government and with state/local personnel.	Yes – Information sharing system must ensure confidentiality of information and protect constitutional and statutory rights of individuals.	Homeland security information.	ISWG, CRS, TIA
14	**Counterintelligence Access to telephone toll and transactional records, 18 USC 2709**	Statute	Access to subscriber information, toll billing records, and electronic communication transactional records, by FBI.	Yes – Requires certification that information is relevant to authorized CI or CT investigation.	Telecommunications subscriber information, toll billing records, and electronic communication transaction records.	CMS/LGL, Markle
15	**USA Patriot Act, National Security Letter authorities**	Statute	USA Patriot Act amendments included clarifications/enhancements to "national security letter" authority under various other statutes.	Yes – Requires relevance to an ongoing terrorism investigation.	Information relevant to a terrorism investigation.	CDT (others included this in references to the underlying statutes)
16	**Privacy Protection Act, 42 USC section 2000aa**	Statute	Prohibits seizure of work product and other documentary materials in exercise of First Amendment rights, subject to certain exceptions.	Yes – Provides protection for First Amendment rights.	Work products and other documentary materials.	G1a
17	**Posse Comitatus Act, 18 USC 1385**	Statute	Prohibits army and air force from executing U.S. laws.	Yes – Prevents military from acting in law enforcement capacity vis-à-vis civilians.	Military.	ISWG, LSG
18	**Use of Information Collected during Military Operations, 10 USC 371**	Statute	Requires DoD to share relevant information with civilian law enforcement officials that may be relevant to a violation of any federal or state law in their jurisdiction.	Yes – Sharing must be in accordance with applicable law.	Information collected during military operations.	LSG

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
19	**Tax Return Information, 26 USC 1063**	Statute	Prohibits disclosure of tax return or return information (very broad definition) by any officer or employee of the U.S., state, local law enforcement agency, local child support enforcement agency or "other person" as defined, except as provided by the provision.	Two of the exceptions apply to the release of terrorist-related information to federal intelligence agencies. Pursuant to section 6103(i)(7)(B), the Secretary of the Treasury may, upon written request, disclose return information (other than information furnished by or on behalf of the taxpayer directly) to federal intelligence agencies that are engaged in the collection or analysis of intelligence and counterintelligence information or investigation concerning any terrorist incident, threat, or activity. In addition, section 6103(i)(7)(C) permits the disclosure of returns and return information to federal intelligence agencies pursuant to an ex parte order by a federal judge. The unauthorized disclosure of returns and return information is subject to civil and criminal sanctions under IRC sections 7431 and 7213. Section 6103 does not differentiate between U.S. and non-U.S. persons with respect to the sharing or release of taxpayer information.	Tax return information.	OMB, WMD 9.4, CRS, TIA
20	**Social Security Information, 42 USC 1306**	Statute	Governs use and disclosure of social security information.	Yes – Prohibits disclosure except as provided by law and regulation.	Social security information.	TAPAC
21	**PL 109-115, Transportation, Treasury, HUD, etc. Act, 2006, 119 Stat. 2503**	Statute	Provision in annual agency appropriation act permanently applicable throughout the government.	Yes – Section 832 prohibits any federal agency from using appropriated funds (funds "made available in this or any other Act") to monitor an individual's use of a federal government Internet site and also prohibits agency from entering into any agreement with a third party to obtain or aggregate personally identifiable information relating to an individual's access to or use of any nongovernmental Internet site. Doesn't apply to voluntary submission of personally identifiable information.	Personally identifiable information from Web site usage.	OMB

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
22	**Census Bureau Information, 13 USC 9**	Statute	Prohibits the use, publication, or examination of any information collected by the U.S. Census Bureau.	Yes – Narrow exceptions – no law enforcement/national security or similar exceptions.	Census data.	CRS, TIA
23	**Family Educational Rights and Privacy Act ("Buckley Amendment"), 20 USC 1232g**	Statute	Requires notice to student/parents if educational records are disseminated – exceptions for investigation of terrorism, with court order on application of AG showing relevance to investigation (1232g(j)).	Yes.	Educational records.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT
24	**Right to Financial Privacy Act, 12 USC 3401 et seq.**	Statute	Restricts use and disclosure of financial records of customers by financial institutions.	Yes. Contains exception for voluntary responses to requests from government authority authorized to conduct CI or FI activities, and for mandatory responses to FBI requests. 12 USC 3414.	Financial records.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT
25	**Fair Credit Reporting Act, 15 USC 1681**	Statute	Restricts use and disclosure of credit report information (1681f), with exception for header information to government agencies, and to government agencies for counterterrorism purposes (1681v).	Yes – Contains exception for counterterrorism purposes, with certification.	Credit report information.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT
26	**Gramm-Leach-Bliley Financial Modernization Act, 12 USC 1811 note**	Statute	Governs collection, sharing of customer information by financial institutions.	Yes – Requires notice, choice, and security safeguards. General exception for sharing in accordance with RFPA and to LE agencies, etc. 15 USC 6802(e).	Financial information.	CMS/LGL, CRS, Markle, TIA, CDT
27	**Bank Secrecy Act of 1970, 12 USC 1892b and 1951-59, and 31 USC 5311-22, and its major component, the Currency and Foreign Transactions Reporting Act, 31 USC 5311-22 (anti-money laundering laws); also FinCEN, 31 USC 310**	Statute	Requires filing of suspicious activity reports and other anti-money laundering measures and reporting, by "financial institutions" broadly defined, and requires DOT to promulgate regulations to ensure that adequate records are maintained of transactions that have a high degree of usefulness in investigatory proceedings. Also establishes FinCEN. The regulations implementing the BSA are set forth at 31 CFR Part 103. In particular, 31 USC § 5319 provides for the sharing of information with the intelligence community, and FinCEN's regulation covering procedures for information sharing authorizes the sharing of BSA information with members of the intelligence community for a national security purpose. See 31 CFR 103.53(d).	Yes – Reports shared with intelligence agencies must be consistent with purpose of subchapter, which includes providing information for FI, CI, and counterterrorism. Treasury regulations must be consistent with Privacy Act and RFPA and must establish guidelines for access and use.	Financial information.	WMD 9.4, CRS, TIA, CDT
28	**Title III and Electronic Communications Privacy Act, 18 USC 2511 et seq, 2701 et seq.**	Statute	Restricts the interception of electronic communications and access to stored communications.	Yes.	Electronic and stored communications.	WMD 9.4, CMS/LGL, CRS, Markle, TIA, CDT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
29	**Telecommunications Act of 1996, 47 USC 153 et seq.**	Statute	Governs provision of telecommunications services.	Yes, section 222 contains certain privacy provisions.	Customer proprietary network information.	CMS/LGL, CRS, TIA
30	**Cable Communications Policy Act of 1984, 47 USC 521 et seq.**	Statute	Section 631 (47 USC 551) covers subscriber privacy — provides for notice, consent, limits on disclosure, government access only pursuant to court order with clear and convincing standard.	Yes.	Cable usage information.	CMS/LGL, CRS, Markle, TIA
31	**Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq.**	Statute	Restricts use and disclosure of state DMV records, with multiple exceptions, including for government official use.	Yes.	DMV records.	CMS/LGL, CRS, TIA
32	**Video Privacy Protection Act of 1988, 18 USC 2710**	Statute	Prohibits disclosure of videotape rental records.	Yes.	Videotape rental records.	CMS/LGL, CRS, Markle, TIA
33	**Health Insurance Portability and Accountability Act of 1996, 42 USC 1320**	Statute	Multiple provisions regarding health insurance portability and fraud.	Yes – Section 264 provides that HHS must promulgate standards with respect to privacy of individually identifiable health information, which were issued as 45 CFR Part 164. The Privacy Rule applies to health care entities, and contains an exemption for disclosure to authorized federal officials for the conduct of lawful intelligence, CI, and national security activities. 45 CFR 164.512.	Individually identifiable health information.	CMS/LGL, CRS, Markle, TIA, CDT
34	**Immigration – Application for Visas, 8 USC 1202**	Statute	Various immigration provisions.	Yes – Prohibits disclosure of Department of State records relating to issuance or refusals of permits for entry to the U.S. Such records are only to be used for administration of immigration, nationality, and other U.S. laws, and otherwise may only be disclosed at the discretion of the Secretary of State to courts and foreign governments under specified circumstances.	Immigration records – visa information.	FGI, CRS
35	**Immigration – Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 USC 1367**	Statute	Various immigration provisions.	Yes – Prohibits disclosure of any information that relates to a person who has filed a claim under the Violence Against Women Act where claim is pending or approved. Exceptions include AG providing for law enforcement purposes.	Immigration records – Claim information filed under Violence Against Women Act.	FGI

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
36	**Immigration – Legalization/ Seasonal Agricultural Work claims, 8 USC 1255a**	Statute	Immigration provisions.	Yes – Prohibits disclosure of information relating to Legalization/Seasonal Agricultural Work claims, with limited law enforcement exception.	Immigration records – Claim information relating to Legalization/ Seasonal Agricultural Work status.	FGI
37	**Immigration – T Visas and U Visas, section 701 of PL 106-386**	Statute	Immigration provisions.	Yes – Restricts disclosure of information relating to trafficking victims (T visas) and victims of crimes (U visas). 8 CFR 214.11(e) enables DHS to provide for law enforcement of those crimes.	Immigration records – victims of crime.	FGI
38	**Immigration – Temporary Protected Status, 8 USC 1254a and 8 CFR 244.166**	Statute	Immigration provisions.	Yes – Restricts DHS disclosure of information relating to temporary protected status of an alien, except for disclosure in course of official duties or for enforcement of INA.	Immigration records – temporary protected status.	FGI
39	**Passenger Manifest Reporting Requirements, 8 USC 1221, 19 CFR 4.7**	Statute	Requirement that aircraft and vessels report to CBP their passenger manifests before arrival in or departure from U.S.	No.	Passenger manifests.	CDT
40	**TSA – Research and Development Activities, 49 USC 40119**	Statute	Research and development to protect passengers and property against piracy, criminal violence, and terrorism.	Yes – Requires Secretary of Transportation to prescribe regulations for restricting disclosures that would constitute an unwarranted invasion of privacy.	TSA R&D information.	FGI
41	**Consolidated Appropriations Act of 2005**	Statute	Requires chief privacy officers and contains other related privacy provisions. Note: applicability unclear to agencies outside of appropriation.	Yes.	Information in possession of covered federal agencies.	OMB
42	**Federal Trade Commission Act, 15 USC 41-58**	Statute	Prohibits unfair or deceptive trade practices and provides FTC with enforcement authority.	Yes – FTC has enforced Act vis-à-vis private sector violations of published privacy policies.	Private-sector data.	CRS
43	**Children's Online Privacy Protection Act, 15 USC 6501**	Statute	Governs Web site collection of information from minors.	Yes.	Web site data collected from children.	CRS, TIA
44	**Child Victims' and Child Witnesses' Rights, 18 USC 3509**	Statute	Nondisclosure provisions for child victims and witnesses.	Yes.	Child victim/witness data.	TIA
45	**Federal Juvenile Delinquency Act, 18 USC 5031 et seq.**	Statute	Nondisclosure provisions for juvenile delinquency records.	Yes – Law enforcement exception.	Juvenile delinquency records.	TIA
46	**Acquisition, Preservation, and Exchange of Identification Records and Information**	Statute	Requires AG to acquire, collect, classify, and preserve identification, criminal identification, crime and other records and exchange with other authorized officials of federal and state agencies for official use.	Yes – Exchange cancelled if recipient shares outside of organization.	Criminal identification information in possession of DOJ.	TIA

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
47	**Alcohol and Drug Abuse Records, 42 USC 290dd-2, and Drug Test Results, PL 100-71, section 503**	Statute	Limits disclosure of alcohol and drug abuse patient records and drug test results.	Yes – Limited exceptions.	Medical information.	TIA
48	**Americans with Disabilities Act and the Rehabilitation Act**	Statute	Improper release of medical information may be considered an act of disability discrimination.	Yes.	Medical information.	TIA
49	**Federal Rule of Criminal Procedure 32**	Federal Rule	Probation officer pre-sentence reports.	Yes – No disclosure without defendant consent, guilty plea, or conviction.	Criminal records.	TIA
50	**EO 12333, United States Intelligence Activities**	Executive Order	Governs intelligence activities.	Yes – Provides rules for collection, retention, and dissemination of U.S. person information.	U.S. person information.	All
51	**EO 13311, Homeland Security Information Sharing**	Executive Order	Assigns to DHS the President's responsibility for procedures under 892(a)(1) of Homeland Security Act.	No.	Homeland security information.	CMS/LGL, CRS
52	**EO 13388, Further Strengthening the Sharing of Terrorism Information Sharing to Protect Americans**	Executive Order	Provides for information sharing to protect against terrorism.	Yes – Requires that agencies give the "highest priority" to, inter alia, the interchange of terrorism information, and in doing so, to protect the freedom, information privacy, and other legal rights of Americans.	Terrorism information.	AT
53	**HSPD 6**	Presiden-tial Directive	Establishes terrorist watch list framework.	Yes – Requires safeguards for USP information.	Terrorist information.	WMD 9.4
54	**Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation.**	AG Memo, Sept 2002	Provides guidance to federal law enforcement for sharing foreign intelligence with the intelligence community. This memorandum applies to the Department of Homeland Security, Department of Justice, and other federal entities having law enforcement responsibilities.	Compilation did not refer to specific privacy provisions – not further reviewed.	Law enforcement information.	ISWG, CMS/LGL, TIA
55	**Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons [Section 203 Guidelines].**	AG Memo, Sept 2002	Specifies procedures for the handling and labeling of information that identifies U.S. persons when sharing such information with the intelligence community.	Yes – This memorandum restricts the ability to share certain types of information afforded by the USA Patriot Act until there is enough information available to determine whether or not the subject of the intercepted information is a U.S. citizen.	Law enforcement information.	ISWG, CMS/LGL, AT

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
56	**Guidelines for FBI National Security Investigations and Foreign Intelligence collection**	AG Guide-lines Oct 2003	Guidelines state as a "general principle" that "the FBI shall provide information expeditiously to other agencies in the intelligence community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions." AG Guidelines also state that consistent with this overriding priority, the FBI shall act in a manner to protect, to the greatest extent possible ... other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. Affirms the MOU on Homeland Security Information Sharing. Authorizes sharing with foreign authorities when in the national security interest, but requires that the FBI consider the reasonably expected effect on any identifiable U.S. person.	Yes – FBI counterintelligence and foreign intelligence information collected under the AG Guidelines, including information acquired in "National Security Investigations" concerning U.S. persons, may be shared with other IC components so they can determine relevance to their responsibilities. However, sharing may be limited to protect security, operational, and prosecutorial interests. In addition, sharing with foreign authorities requires considering the effect on any identifiable U.S. person.	FBI foreign intelligence and counterintelligence.	ISWG, AT
57	**Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations**	AG Guide-lines May 2002	Governs FBI investigations of terrorism enterprises.	Yes – USP rules.	FBI information.	CRS, TAPAC, TIA
58	**Guidelines Applicable to FBI Foreign Counterintelligence Investigations**	AG Guide-lines	Governs FBI foreign CI investigations.	Yes.	FBI information.	TIA
59	**DOJ – Criminal Intelligence System Operating Policies, 28 CFR Part 23**	DOJ Regula-tions	Provisions for assuring that all criminal intelligence systems operating under Omnibus Crime Control and Safe Streets Act are utilized in conformance with the privacy and constitutional rights of individuals.	Yes – 28 CFR 23.20 sets forth "operating principles" to protect privacy and constitutional rights, such as ensuring information is based on reasonable suspicion, no information is in violation of law, dissemination based on need to know, etc.	Criminal intelligence.	G1a
60	**DOJ – The National Criminal Intelligence Sharing Plan**	DOJ Guidance	The National Criminal Intelligence Sharing Plan ('Plan') is a formal intelligence sharing initiative that addresses the security and intelligence needs recognized after the tragic events of September 11, 2001. It describes a nationwide communications capability that will link together all levels of law enforcement personnel, including officers on the streets, intelligence analysts, unit commanders, and police executives for the purpose of sharing critical data.	Yes – Contains guidance for creating privacy policies and for protecting privacy, civil liberties, and civil rights during information sharing.	Criminal intelligence.	G1a

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
61	**DOJ – Justice Information Privacy Guideline**	DOJ Guidance	Referenced in the NCISP – a guideline for developing, drafting, and assessing privacy policy for justice information systems (criminal and civil justice systems across the board, not DOJ centric).	Yes – Provides guidance on developing privacy policy for civil and criminal justice systems.	Information in civil and criminal justice systems.	G1a
62	**DOJ – Privacy Policy Development Guide**	DOJ Guidance	Developed by Global Privacy and Information Quality Working Group of DOJ's Global Justice Information Sharing Initiative.	Yes – Provides guidance on developing privacy policies to protect personal information in a sharing environment.	Information in civil and criminal justice systems.	G1a
63	**DOJ/DHS – Fusion Center Guidelines**	DOJ-HS Guidance	Guidelines for establishing and operating fusion centers at the local, state, tribal, and federal levels.	Yes – Guideline 8 is to develop, publish, and adhere to a privacy and civil rights policy. Provides guidance on developing policies – refers to Justice Information Privacy Guideline.	Law enforcement intelligence.	G1a
64	**National Instant Criminal Background Check System, DOJ Regulations, 28 CFR Part 25**	DOJ Regula-tions	Procedures for implementing the Brady Act referencing instant criminal background check for firearms transfers.	Yes – Access prohibited for any purpose other than issuance of firearms licenses and enforcement of the Gun Control Act.	Criminal background records.	WMD 9.4
65	**DOJ/FBI – Production or Disclosure of Material, 28 CFR part 16**	FBI Regula-tions	Regulations for disclosing FBI records, including under Privacy Act, in litigation, and on request of subject.	Yes.	Law enforcement.	G1a
66	**FBI Policy for Law Enforcement Sensitive Marking, Letter from FBI Deputy Director to Deputy Secretary of Defense**	FBI Policy	The "Law Enforcement Sensitive" (LES) marking indicates that information was compiled for law enforcement purposes and should be afforded appropriate security to protect specified law enforcement interests. Such information generally is not classifiable. It is to be entrusted only to those persons within an agency who have demonstrated a legitimate need to know the information. It is to be safeguarded in accordance with Justice Department requirements for information marked" Limited Official Use" and is the type of information exempt from disclosure under FOIA Section 552(b).	Compilation did not refer to specific privacy provisions – not further reviewed.	Law enforcement information.	WMD 9.4
67	**FBI Standard FISA Minimization Procedures (various)**	AG – approved Proce-dures	Sets forth procedures for minimizing U.S. person information collected under FISA.	Yes.	Intelligence information collected under FISA.	WMD 9.4

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
68	**Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security concerning Information Sharing**	MOU March 2003	Prescribes policies and procedures for sharing terrorism information.	Yes – "All information sharing pursuant to this Agreement shall be consistent with applicable privacy laws."	Terrorism information.	ISWG, WMD 9.4, CMS/LGL
69	**Memorandum of Understanding on the Integration and use of Screening Information to Protect Against Terrorism (TSC MOU); and Addendum A**	MOU	Prescribes policies and procedures for terrorist screening information and the Terrorist Screening Center.	Yes – Procedures must be developed to address repeated misidentification, regularly correct information, and protect personal privacy.	Terrorist information.	WMD 9.4
70	**DCID 2/5 – TTIC**	DCI Directive	Establishes TTIC.	Yes – Requires agency assignees to continue to comply with their own legal authorities and restrictions and all applicable statutes and EOs, "including those relating to the protection of Constitutional rights and privacy."	Terrorist threat-related information.	CMS/LGL
71	**DCID 8/1 – Information Sharing**	DCI Directive	Requires expanded information sharing by intelligence community.	No.	Intelligence information.	CMS/LGL
72	**DoD 5240.1, DoD Intelligence Activities**	DoD Directive	Governs DoD Intelligence Activities.	Yes – Lays out general governing principles/restrictions; refers to 5240.1-R.	Intelligence information.	ISWG
73	**DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons [also note classified SIGINT annex]**	DoD Directive	Limits, and provides procedures for, collection, retention, use, and dissemination of information about U.S. persons.	Yes – Imposes strict limits on information that may be collected or retained about U.S. persons. Severely limits information that can be received from law enforcement and the fluidity with which information can be shared. Permitted to disseminate to: (1) DoD employee needing it for duties; (2) appropriate F/S/L law enforcement; (3) agency within intelligence community; (4) federal agency authorized to receive in relation to its duties; (5) foreign government authorized under agreement. May also share incidentally-acquired information with F/S/L law enforcement re: violation of law.	Intelligence information.	ISWG

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
74	**DIA Regulation 60-4 Procedures Governing DIA Intelligence Activities That Affect U.S. Persons**	DIA Regula-tion	Outlines authorities and procedures in conducting intelligence activities that may affect U.S. persons, to include identifying and reporting questionable activities.	Yes – Restricts the collection, retention, and dissemination of information concerning U.S. persons.	Intelligence information.	ISWG
75	**USSID 18 – Legal Compliance and Minimization Procedures**	NSA Regula-tion	Governs collection, retention, dissemination of information by NSA.	Yes.	Intelligence information.	ISWG, WMD 9.4
76	**Standard Minimization Procedures for NSA Electronic Surveillances [FISA]**	NSA Regula-tion	Required by FISA.	Yes – Procedures for minimizing USP information under FISA.	FISA information.	WMD 9.4
77	**DCI Memorandum on Procedures for Dissemination of Intelligence Referring to Members of Congress and Their Staffs ("Gates Procedures")**	DCI Directive	Restrictions on dissemination of identity information re Congress members/staffs.	Yes.	Intelligence information.	WMD 9.4
78	**Imagery Policy Series**	NGA Regula-tion	Imagery guidelines and restrictions.	Document referenced in compilation but not described – not further reviewed.	Imagery.	ISWG
79	**DODD 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense**	DoD Directive	Applies to non-intelligence DoD elements. Sets out numerous restrictions pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the Department of Defense.	Yes – Prohibits certain types of otherwise legal collection, storage, and dissemination of information. Requires high-level approval of certain other types.	Information in possession of DoD.	ISWG
80	**DoD Directive 1304.23, Acquisition and Use of Criminal History Record Information by the Military Services, November 16, 1994**	DoD Directive	Criminal background information on DoD applicants.	Yes – Requires confidentiality of records, use only for applicant review purposes.	Criminal background records.	G1a
81	**DoD Directive 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, November 3, 2005**	DoD Directive	Rules for intelligence interrogations, etc.	Yes – Medical information of detainees must be handled with respect for patient privacy.	Medical information of detainees.	G1a
82	**DODD 5400.11, DoD Privacy Program (see also 5400.11-R)**	DoD Directive	Policy and procedures to implement Privacy Act to maintain privacy of personal information on individuals held in a system of records maintained by a Component.	Prohibits release of personal information on individuals held in a system of records maintained by Component, with limited exceptions [Does not refer to 5240.1-R].	DoD Privacy Act information.	ISWG
83	**DODD 5525.5, DoD Cooperation with Civilian Law Enforcement Officials**	DoD Directive	Policy encouraging cooperation with F/S/L law enforcement.	Refers to 5420.1-R and 5400.11, among others.	Information in possession of DoD.	ISWG

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
84	**DODD 2000.12, DoD Antiterrorism Program, 18 Aug 2003**	DoD Directive	Establishes responsibilities within DoD regarding antiterrorism; inter alia, requires "fusing" of information and "suspicious activity reporting" from law enforcement, CI, and other sources.	No.	Information in possession of DoD.	G1a
85	**DoD Regulation 6025.18-R, DoD Health Information Privacy Regulations, January 24, 2003**	DoD Regulation	Implements HIPAA privacy rule.	Yes – Governs use and disclosure of health information.	Personally identifiable health information.	G1a
86	**DoD – Joint Pub (JP) 3-07.2 Joint Tactics, Techniques, and Procedures for Anti-terrorism, 1998**	DoD Guidance	Provides guidance for DoD antiterrorism measures.	Yes – Contains legal guidance for use of military in antiterrorism situations, including legal guidance for domestic situations.	Military.	G1a
87	**DoD Strategy for Homeland Defense and Civil Support**	DoD Strategy	Support homeland defense.	Yes – Actions must be consistent with privacy protections and constitutional authorities.	Information in possession of DoD.	G1a
88	**AF Instruction 14-104, Oversight of Intelligence Activities**	Air Force Instruction	Air Force regulation for intelligence oversight.	Yes – USP rules.	USP information.	WMD 9.4
89	**AF Policy Directive – AFPD 71-1, Criminal Investigations and Counterintelligence**	Air Force Policy	Governs criminal investigations and CI to protect AF personnel and facilities.	Yes – Reference to USP rules.	Information in possession of USAF.	G1a
90	**Army Regulation 381-10, U.S. Army Intelligence Activities**	Army Regulation	Army regulation for intelligence activities.	Yes – USP rules.	USP information.	WMD 9.4
91	**Secretary of the Navy Instruction 381-10, Oversight of Intelligence Activities within the Department of the Navy**	Navy Instruction	Navy regulation for intelligence oversight.	Yes – USP rules.	USP information.	WMD 9.4
92	**CIA HR 7-1, Law and Policy Governing the Conduct of Intelligence Activities**	CIA Regulation and AG Guidelines	Classified regulation – contains AG guidelines under EO 12333 and imposes other restrictions.	Yes.	USP information.	CMS/LGL
93	**Department of Energy Procedures for Intelligence Activities (with supplements)**	DOE Regulation and AG Guidelines	Contains AG guidelines under EO 12333.	Yes.	USP information.	WMD 9.4

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
94	**OMB – Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948 (July 9, 1975)**	OMB Guide-lines	Amplifies on all Privacy Act terms and provisions, including limitations on and requirements for disclosure of identifiable information outside the agency.	Yes.	Privacy Act information.	OMB
95	**OMB – Privacy Act Guidance – Update (May 24, 1985)**	OMB Guide-lines	Supplemental guidance addressing using use of Privacy Act info in the litigation context and relationship of Privacy Act to FOIA (non-consensual disclosure of info where FOIA requires).	Yes.	Privacy Act information.	OMB
96	**OMB – Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 FR 25818 (June 16, 1989)**	OMB Guide-lines	Explains content of and procedures for conducting cost-benefit analyses and publishing inter-agency agreements preliminary to conducting computer matches.	Yes.	Privacy Act information.	OMB
97	**OMB – Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974, 56 FR 18599 (April 23, 1991)**	OMB Guide-lines	Addresses verification procedures (due process requirements) preliminary to decision-making about individual rights, benefits or privileges based on information derived from computer matching activities.	Yes.	Privacy Act information.	OMB
98	**OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, Appendix 1 (November 28, 2000)**	OMB Guide-lines	Amplifies on statutory (Privacy Act) requirements for publication of Privacy Act Systems of Records Notices and Computer Matching Agreements that implicate disclosure of records outside the agency.	Yes.	Privacy Act information.	OMB
99	**OMB Circular A-16, Coordination of Geographic Information and Related Spatial Data Activities (August 19, 2002) (incorporates EO 12906)**	OMB Guide-lines	Describes the responsibility of agencies to collect, share, and disseminate spatial data among all levels of government.		Special data.	OMB
100	**OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB Memorandum 03-22, February 2004)**	OMB Guide-lines	Articulates requirement to conduct or update Privacy Impact Assessment where a system change creates new privacy risks, e.g., application of new technologies, matching, merging or centralization of databases, incorporation of commercial source information, new interagency uses (e.g., where agencies work on shared functions involving significant new uses or exchanges of information in identifiable form, alternation of business process, alteration in character of data).	Yes.	E-Government Act.	OMB

	Rule	Type of Rule	Summary	Privacy/Civil Liberties Provisions?	Data Type	Source
101	**OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000)**	OMB Guide-lines	Prohibiting the use of persistent cookies to track an individual's activity on Internet; prohibition on use of "tracking technology" in general is picked up in OMB Memorandum 03-22, above.	Yes.	Federal Web site usage data.	OMB
102	**OMB Memorandum M-05-08, February 2005**	OMB Guide-lines	Requests appointment of "senior agency officials for privacy" and lays out other privacy expectations.	Yes.	Personally identifiable information in possession of agency.	OMB
103	**DOJ – Law Enforcement Information Sharing Plan (LEISP)**	DOJ Policy	National strategy developed by state/local law enforcement personnel to enhance intelligence-based policing.	Document referenced in compilation but not described – not further reviewed.	Law enforcement information.	G1a
104	**Department of Homeland Security Management Directive Number 11042.1, "Safeguarding Sensitive but Unclassified ('For Official Use Only') Information," January 6, 2005**	DHS Directive	DHS rules for FOUO information.	Yes – Requires FOUO designation for information exempt from disclosure under the Privacy Act, or the disclosure of which could adversely affect a person's privacy.	DHS information.	G1a
105	**DHS Privacy Act Procedures, 6 CFR Part 5**	DHS Regula-tions	DHS Privacy Act regulations.	Yes.	DHS Privacy Act information.	G1a
106	**FBI Name Check Program**	Inter-agency agreement	Interagency agreement to share information with the FBI.	Document referenced in compilation but not described – not further reviewed.	Document referenced in compilation but not described – not further reviewed.	G1a
107	**FINCEN MOU**	Inter-agency agreement	Provides data related to financial crimes shared via Treasury.	Document referenced in compilation but not described – not further reviewed.	Financial data.	G1a
108	**Fingerprint Cards & Name Checks**	Inter-agency agreement	Interagency agreement to share information with the FBI.	Document referenced in compilation but not described – not further reviewed.	Document referenced in compilation but not described – not further reviewed.	G1a
109	**Visa Processing MOU**	Inter-agency agreement	Interagency agreement to share information with the FBI.	Document referenced in compilation but not described – not further reviewed.	Document referenced in compilation but not described – not further reviewed.	G1a